EXHIBIT A

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

BUBBLE GUM PRODUCTIONS, LLC,

Plaintiff,

v.

DOES 1 – 37,

Defendants.

CASE NO. 1:12-cv-00595

Judge: Honorable Joan H. Lefkow
Magistrate: Honorable Susan E. Cox

DECLARATION OF PETER HANSMEIER IN SUPPORT OF MOTION FOR LEAVE TO TAKE DISCOVERY PRIOR TO RULE 26(f) CONFERENCE

I, Peter Hansmeier, declare under penalty of perjury as true and correct that:

1. I am a technician at 6881 Forensics, LLC ("6881"). On behalf of its clients, 6881 monitors and documents Internet-based piracy of our clients' copyrighted creative works. I submit this declaration in support of Plaintiff's Motion for Leave to Take Discovery Prior to Rule 26(f) Conference.

2. The Plaintiff in this action is the exclusive rights holder of the right to distribute and reproduce certain copyrighted creative works via the BitTorrent protocol. We have been engaged to collect and document evidence of the unauthorized reproduction and distribution of the copyrighted creative works, including the works referenced in Exhibit A to the Complaint, within the United States of America. As a technician at 6881, I am responsible for implementing day-to-day piracy monitoring.

3. This affidavit is based on my personal knowledge, and if called upon to do so I would be prepared to testify as to its truth and accuracy.

Background

4. The Internet is a global network of devices and networks that are connected to one another via a worldwide communications infrastructure. As with any tool, the Internet is put to uses both good and bad.

5. One undesirable use of the Internet is content piracy. Over the past decade, the ease of creating exact digital reproductions of copyrighted albums, audiovisual works, software, photographs and other forms of media has increased dramatically. Indeed, a significant amount of content, including Plaintiff's creative works, is published exclusively in digital format, which increases the public's access to digital reproductions. While access to digital reproductions of copyrighted media has increased, the costs of digital storage capacity and internet bandwidth have fallen precipitously. The combination of increased access to digital content and the lower costs of storage and transmission of that content over the Internet has created a situation ripe for systemic Internet-based content piracy.

6. A development that heralded the arrival of wide scale Internet-based piracy was the introduction of modern peer-to-peer file transfer protocols. Under earlier file transfer protocols, users downloaded data directly from a central server. The rate of data transmission provided by a central server would slow dramatically when the large numbers of users requested data simultaneously. Moreover, central servers that distributed pirated content were vulnerable to legal injunctions.

7. Modern peer-to-peer file transfer protocols substantially avoid these problems by allowing each data-seeking user to both upload to and download from other data-seeking users without the material assistance of a robust central server. In contrast to traditional file transfer protocols, modern peer-to-peer protocols actually work *better* when large numbers of users

request data simultaneously because as the number of users seeking a file grows, so too does the number of users from which to download the file. Moreover, a distributed web of users is far more difficult to shut down than a central server.

8. The most popular peer-to-peer file transfer protocol is the BitTorrent protocol. Studies have estimated that the BitTorrent protocol accounts for up to 70% of all peer-to-peer traffic and as much as 50% of all Internet traffic in some parts of the world. In BitTorrent vernacular, individual downloaders of a file are called peers. The aggregate group of peers involved in downloading a particular file is called a swarm. A server that stores a list of peers in a swarm is called a tracker. A computer program that implements the BitTorrent protocol is called a BitTorrent client.

9. The sharing of a file via the BitTorrent protocol operates as follows. First, a person who possesses a complete digital reproduction of a given file intentionally elects to share the file with other Internet users. That complete file is called a "seed." The initial "seeder" creates a small "torrent" file that contains instructions for how to find the seed. The seeder uploads the torrent file to one or more of the many torrent indexing sites. As Internet users come across the torrent file, they intentionally elect to load the torrent files in their BitTorrent client, which uses the instructions contained in the torrent file to locate the seed. These users now are peers in a swarm with respect to that digital reproduction. The BitTorrent protocol dictates that each peer download a random portion of the file (a "piece") from the seed. After a peer has downloaded its first piece, it then shares that piece and subsequent pieces with other peers in the swarm. The effect of this protocol is that each peer is both a downloader and uploader of an illegally-transferred file. As more peers join the swarm, the rate of data transfer typically increases because the odds of connecting to another peer improve.

10. In observing the swarms that were formed to distribute the copyrighted content subject to Plaintiff's exclusive rights, I observed swarms that were hundreds of users large that contained peers from states across the United States as well as many countries around the world. The BitTorrent protocol is particularly well suited to transferring large files, such as the audiovisual works produced by Plaintiff, as it allows even small computers with low bandwidth to be capable of participating in large data transfers across a peer-to-peer network.

11. Where, as here, a content owner such as Plaintiff has not authorized this uncontrolled mass-reproduction and distribution of its content via the BitTorrent protocol, I believe that the copying and distribution of its content violates copyright laws. Because BitTorrent is a distributed protocol, there is no central server that can be targeted for purposes of stemming the tide of piracy. I believe that seeking recourse against individual content pirates is likely to be the most effective means of addressing BitTorrent-based content piracy.

Identification of the Doe Defendants

12. In order to assist Plaintiff in identifying instances of copyright infringement on BitTorrent-based peer-to-peer networks, 6881 used sophisticated and proprietary peer-to-peer network forensic software to perform exhaustive real time monitoring of BitTorrent-based swarms involved in distributing the copyrighted creative works relevant to Plaintiff's action. 6881's proprietary software is effective in capturing granular-level data about the activity of peers in a swarm and their infringing conduct and 6881's processes are designed to ensure that information gathered about each Doe Defendant is accurate.

13. The first step in the infringer-identification process is to locate swarms where peers are distributing the copyrighted creative works. I accomplished this step by using a variety of techniques to locate torrent files sharing the names of copyrighted creative works subject to

Plaintiff's exclusive rights. Such files are commonly located on torrent indexing sites, but can also be found on Internet file-sharing forums and areas where users congregate. Because a torrent file only contains directions about where to find the swarm associated with a particular item of digital content, the next step is to locate the swarm.

14. The most common means of locating a swarm is to connect to a BitTorrent tracker, which is a server that contains an updated list of peers in a swarm. A typical torrent file contains a list of multiple trackers associated with the underlying file. Other means of locating a swarm include using Distributed Hash Tables, which allow each peer to serve as a "mini-tracker" and Peer Exchange, which allows peers to share data about other peers in the swarm without the use of a tracker. I used all three methods to locate swarms associated with Plaintiff's exclusive rights.

15. After locating a swarm, I used 6881's proprietary forensic software to conduct an exhaustive real time "fingerprint" of the swarm. In doing so, I collected data on the peers in the swarm, including what activities each peer was engaging in and other important data such as the date and time that each Defendant was observed by the software as engaging in infringing activity and each Defendant's Internet protocol ("IP") address at that date and time. Although I was able to observe Defendants' infringing activity through forensic software, this system does not allow me to access Defendants' computers to obtain identifying information other than an IP address. Nor does this software allow me to upload a file onto Defendant's computer or otherwise to communicate with it.

16. An IP address is a unique number that is assigned to Internet users by an Internet service provider at a given date and time. There are two types of IP addresses: dynamic and static. A static IP address is an IP address that will be associated with a particular user as long as

that user is a customer of a given Internet service provider. A dynamic IP address is an IP address that will change from time-to-time.

17. Most consumer customers of Internet service providers are assigned a dynamic IP address. The reason for this is that an Internet Service provider can get by with a smaller overall pool of IP addresses if it simply assigns the next available IP address at a given time to a customer who wishes to connect to the Internet versus allocating a permanent and unquiet IP address to each of its users. Internet service providers keep logs of IP addresses, but the length of time they keep the logs can be as short as days, making expedited discovery of the identities associated with those IP addresses critically important in the instant action, particularly since nearly all of the Defendants I observed appeared to be associated with dynamic IP addresses.

18. After recording granular level data about every peer in the swarm, the next step is to carefully and thoroughly review the data produced by 6881's proprietary forensic software to determine what peers were actually involved in illegally reproducing and distributing our client's copyrighted creative works. We then trace each offending IP address to specific ISPs. I performed this work with respect to the copyrighted creative content subject to Plaintiff's exclusive rights.

19. When a verified peer was located who was making files subject to Plaintiff's license available for distribution and reproduction via the BitTorrent protocol, I downloaded and retained both the torrent files and the actual digital reproductions being offered for distribution to verify that the digital copies being distributed in the swarm were in fact copies of the copyrighted creative works subject to Plaintiff's license. Because a file could be mislabeled, corrupt or otherwise not an actual copy of Plaintiff's files, I physically downloaded the file and compared it

to an actual copy of the copyrighted creative works to confirm that the file was a substantially-similar reproduction of the copyrighted creative work.

20. Finally, I stored all of the data we collected in a central database for later use, examination and audit.

The Critical Importance of Expedited Discovery

21. Defendants are known to Plaintiffs only by the IP number they were assigned by their Internet service provider on the date and time we observed each Defendant engaging in infringing conduct. The only party from whom Plaintiff can discover Defendant's actual names and addresses is Defendant's Internet service provider. Without expedited discovery in this case against Defendant's Internet service provider, Plaintiff will have no means of serving Defendants with the complaint and summons in this case and no means to protect its creative works from ongoing infringement.

22. Internet services providers have different policies regarding the length of time they preserve information about what IP address was associated with a given subscriber at a given date and time. Some Internet service providers store this information for as little as weeks or even days before potentially permanently erasing the data they contain. Informal requests for data preservation to Internet service providers can meet with varying degrees of success and are no substitute for formal discovery. If an Internet service provider does not have to respond efficiently to a discovery request, the information in that ISP's database may be erased forever.

23. Certain ISPs own excess IP addresses that they lease or otherwise allocate to third party "intermediary ISPs." Because the lessor ISP has no contractual relationship with the intermediary ISP's customers, the leasing ISP would be unable to identify the Doe Defendants

through reference to their user logs. In contrast, the intermediary ISP should be able to so identify.

Continued Monitoring

24. The copyrighted creative works at the heart of this action continue to be made available for unlawful duplication and distribution via the BitTorrent protocol, in violation of Plaintiff's exclusive rights to reproduce and distribute the copyrighted works via the BitTorrent protocol. 6881 continues to monitor on a real time basis the unlawful duplication and distribution and to identify content pirate by the unique IP address assigned to them by their respective Internet Service Providers on the date and at the time of the infringing activity.

Executed on February 15, 2012, in Minneapolis, MN.

_____

Peter Hansmeier